

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年11月 5日

出 願 番 号
Application Number:

特願2002-321355

[ST.10/C]:

[JP 2002-321355]

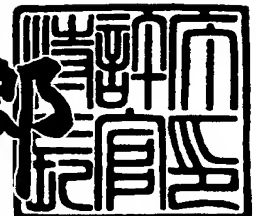
出 願 人
Applicant(s):

株式会社東芝

2003年 1月31日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3002814

【書類名】 特許願

【整理番号】 A000205169

【提出日】 平成14年11月 5日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明の名称】 通信装置及び通信方法

【請求項の数】 20

【発明者】

 【住所又は居所】 東京都青梅市末広町 2 丁目 9 番地 株式会社東芝青梅事業所内

 【氏名】 小久保 隆

【発明者】

 【住所又は居所】 東京都青梅市末広町 2 丁目 9 番地 株式会社東芝青梅事業所内

 【氏名】 奥山 武彦

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置及び通信方法

【特許請求の範囲】

【請求項 1】

非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施すパディング処理部と、

前記パディング処理部によりパディング処理されたパディング非同期パケット及び同期パケットを暗号化する暗号部と、

前記暗号部により暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信する送信部と、

を具備することを特徴とする通信装置。

【請求項 2】

前記非同期パケットの実データの長さに関するデータ長情報を、前記暗号化パディング非同期パケットに付加するデータ長情報付加回路を更に有する請求項 1 記載の通信装置。

【請求項 3】

前記暗号部で行う暗号化処理に用いる鍵情報を鍵書換情報に基づいて書き換え、前記鍵書換情報を前記暗号化パディング非同期パケットに付加する鍵管理部を更に有する請求項 1 記載の通信装置。

【請求項 4】

少なくとも前記非同期パケットのコピー回数を制限するコピー制御情報を、前記暗号化パディング非同期パケットに付加するコピー制御情報付加回路を更に有する請求項 1 記載の通信装置。

【請求項 5】

前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号部で行う暗号化処理に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして、前記暗号化パディング非同期パケットの列の中に挿入する付加回路を更に有する請求項 1 記載の通信装置。

【請求項 6】

前記送信部から送信された前記暗号化パディング非同期パケットを受信する受信部と、

前記受信部が受信した前記暗号化パディング非同期パケットを復号して、前記パディング非同期パケットを出力する復号部と、

前記復号部が出力した前記パディング非同期パケットから、前記パディング処理部で付加したデータを除いて実データを抽出する抽出部と、

を具備することを特徴とする請求項 1 記載の通信装置。

【請求項 7】

前記抽出部は、前記非同期パケットの実データの長さに関するデータ長情報を検出し、これに基づいて、前記復号部が出力した前記パディング非同期パケットから、前記付加したデータを除いて実データを抽出することを特徴とする請求項 6 記載の通信装置。

【請求項 8】

前記復号部は、前記暗号部で行う暗号化処理に用いる鍵情報を書き換える鍵書換情報を検出し、これにより書き換えた最新の鍵情報に基づいて、前記受信部が受信した前記暗号化パディング非同期パケットを復号することを特徴とする請求項 6 記載の通信装置。

【請求項 9】

前記受信部が受信した前記非同期パケットのコピー回数を制限するコピー制御情報を検出し、この制限の範囲内で、少なくとも前記非同期パケットをコピーするコピー機能を更に有する請求項 6 記載の通信装置。

【請求項 10】

前記受信部は、前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号部で行う暗号化処理に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして受信することを特徴とする請求項 6 記載の通信装置。

【請求項 11】

非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施し、

前記パディング処理されたパディング非同期パケット及び同期パケットを暗号化し、

前記暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信することを特徴とする通信方法。

【請求項 1 2】

前記非同期パケットの実データの長さに関するデータ長情報を、前記暗号化パディング非同期パケットに付加することを特徴とする請求項 1 1 記載の通信方法。

【請求項 1 3】

前記暗号化に用いる鍵情報を鍵書換情報に基づいて書き換え、前記鍵書換情報を前記暗号化パディング非同期パケットに付加することを特徴とする請求項 1 1 記載の通信方法。

【請求項 1 4】

少なくとも前記非同期パケットのコピー回数を制限するコピー制御情報を、前記暗号化パディング非同期パケットに付加することを特徴とする請求項 1 1 記載の通信方法。

【請求項 1 5】

前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号化に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして、前記暗号化パディング非同期パケットの列の中に挿入することを特徴とする請求項 1 1 記載の通信方法。

【請求項 1 6】

前記送信された前記暗号化パディング非同期パケットを受信し、これを復号して、前記パディング非同期パケットを出力し、

前記パディング非同期パケットから前記付加したデータを除いて実データを抽出することを特徴とする請求項 1 1 記載の通信方法。

【請求項 1 7】

前記非同期パケットの実データの長さに関するデータ長情報を検出し、これに基づいて、前記復号されたパディング非同期パケットから、前記付加したデータを除いて実データを抽出することを特徴とする請求項 1 6 記載の通信方法。

【請求項 1 8】

前記暗号化に用いる鍵情報を書き換える鍵書換情報を検出し、これにより書き換えた最新の鍵情報に基づいて、前記受信した前記暗号化パディング非同期パケットを復号することを特徴とする請求項 1 6 記載の通信方法。

【請求項 1 9】

前記非同期パケットのコピー回数を制限するコピー制御情報を検出し、この制限の範囲内で、少なくとも前記非同期パケットをコピーすることを特徴とする請求項 1 6 記載の通信方法。

【請求項 2 0】

前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号化に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして受信することを特徴とする請求項 1 6 記載の通信方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、パケット通信を行う通信装置であって、特に、非同期パケットを暗号化してパケット通信を行う通信装置及び通信方法に関する。

【0 0 0 2】

【従来の技術】

最近、多様なデジタル機器の開発・普及が広範に進み、これに応じて、デジタル機器同士の通信機能への要望も高まりつつある。すなわち、例えば、I E E E (Institute of Electrical Electronics Engineers) 1 3 9 4 等の通信機能をもった D T V (Digital Television) や D V D (Digital Versatile Disk) プレイヤ等が一般化してきている。

【 0 0 0 3 】

これに関連した従来技術として、扱うデジタル情報の複写機能をもったデジタル機器を示す例がある（例えば、特許文献 1 参照）。ここでは、所定のデータフォーマットからコピー世代管理情報を検出する手段と、所定のデータフォーマットをネットワークバスのパケットフォーマット変換手段を含み、検出したコピー管理情報を変換手段による変換後のパケットフォーマットの所定位置に挿入してネットワークバスに送出する送信側インタフェースをもったデジタル機器が示されている。ここでは、同期式パケットとは明言されていないが、一例として、IEEE 1394 の同期パケットに適用するものと考えられる。

しかしながら、ここでは、非同期パケットを暗号化する手法が述べられてはいない。従って、D T C P (Digital Transmission Content Protection) 暗号化方式等で同期パケットを暗号化している場合、非同期パケットの情報（例えば、画像情報等）については、同期パケットと一緒に暗号化を行うことができないため、セキュリティを保つことができない。

【 0 0 0 4 】

【特許文献 1】

特開平 0 8 - 1 8 4 8 8 1 号公報。

【 0 0 0 5 】

【発明が解決しようとする課題】

すなわち、従来の通信装置においては、同期パケットに施されるブロック暗号等の暗号処理を、データ長が異なるために非同期パケットにはそのまま用いることができないので、同期パケットと非同期パケットが混在するデジタル機器においては、同期パケットのみについてブロック暗号が施され、非同期パケットは暗号化されることなく通信されてしまう。これにより、非同期パケットについては、第三者による不正複写に対してセキュリティが保てないという問題がある。

本発明は、非同期パケットも同期パケットと同様に暗号化して通信を行う通信装置及び通信方法を提供することを目的とする。

【 0 0 0 6 】

【課題を解決するための手段】

本発明は、非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施すパディング処理部と、前記パディング処理部によりパディング処理されたパディング非同期パケット及び同期パケットを暗号化する暗号部と、前記暗号部により暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信する送信部とを具備することを特徴とする通信装置である。

【 0 0 0 7 】

D T C P 暗号化方式のように一定のブロック長によるブロック暗号により、同期パケットを暗号化して、I E E E 1 3 9 4 等で他のデジタル機器と通信を行っているデジタル機器において、非同期パケットは、一定のブロック長をもっていないので、一律には暗号化処理を行うことができない。本発明に係る通信装置では、パディング処理により非同期パケットの実データに無効データ等を付加することで、暗号化方式が必要とするブロック長をもたせることにより、非同期パケットも同期パケットと同様に暗号化することができる。これにより、非同期パケットによりデータも同期パケットと同様に暗号化して、他のデジタル機器との間の通信を行うことが可能となる。

【 0 0 0 8 】

【発明の実施の形態】

以下、図面を参照してこの発明の実施形態である通信装置を詳細に説明する。図 1 は、本発明に係る通信装置であるテレビジョンの構成の一例を示すブロック図、図 2 は、本発明に係る通信装置により非同期パケットに施されるパディング処理を説明する図、図 3 は、パディング処理された非同期パケットに制御情報を付加することを説明する図、図 4 は、パディング処理された非同期パケットに制御情報の専用非同期パケットを付加することを説明する図、図 5 は、非同期パケットをパディング処理して送信処理する動作を説明するフローチャート、図 6 は、パディング処理された非同期パケットを受信処理する動作を説明するフローチャート、図 7 は、本発明に係る通信装置により構成されたネットワークシステムの一部を示すシステム図である。

【 0 0 0 9 】

＜通信装置とネットワークシステムの構成＞

本発明に係る通信装置は、例えば、デジタルテレビ等のデジタル機器であり、例えば、IEEE 1394等の通信機能をもった通信装置である。ここでは、転送される情報はパケット形式で扱われ、同期パケットと非同期パケットとに分けることができる。

【0010】

図1において、通信装置N2は、デジタルテレビの本来の機能、すなわち、同調回路や復号回路、映像処理回路や、オーディオ増幅部等の働きを総称する信号処理部11と、映像を表示するための表示部10との他に、通信機能として、ブロック暗号化処理をおこなうDTC P部12と、これに含まれる非同期パケット・鍵管理部13とを有している。更に、通信装置N2は、先の信号処理部11とDTC P部12とにデータバスでそれぞれ接続されており、送信すべき非同期パケットを扱う非同期処理部／パディング処理部14と、受信した非同期パケットを扱う非同期処理部／抽出部15と、同期パケットを扱う同期処理部16と、パケットにデータ長情報及びコピー情報等を付加するためのデータ長情報・コピー情報付加回路17と、送信部・受信部18とを有している。

又、更に、本発明に係る通信装置は、ネットワークNで複数のデジタル機器にそれぞれ接続されるネットワークを構成するものであり、図7のシステム図は、このネットワークを示している。すなわち、本発明に係る通信装置は、図7において、ネットワークNにそれぞれ接続される、DVDプレイヤーN1と、DTV N2と、PC (Personal Computer) N3と、DTV N4と、DVHS N5と、プリンタN6とにより構成されるネットワークシステムに適用することができる。

【0011】

ここでは、一例として、IEEE 1394を通信規約とするパケット通信を行っているが、この通信規約に限ることなく、他のネットワーク通信の通信規約を用いるものであっても可能である。

＜本発明に係る通信動作及びパディング処理動作＞

次に、上述した本発明に係る通信装置の通信動作及び本発明に特有のパディング処理動作を、パケットを示すタイミングチャート及びフローチャートを用いて

詳細に説明する。

初めに、同期パケットと非同期パケットとの相違について述べる。同期パケットは、主に、動画映像データや音声データであることが多く、パケットの伝送に時間上の制約がある。又、送信側と受信側とで時刻あわせができる。又、リアルタイムの伝送用パケットであり、パケットの実データ部分の長さが固定値の整数倍である等の特徴をもっている。又、非同期パケットは、主に、制御データや静止画データであり、時刻の制約はなく、非リアルタイム伝送であり、可変調であるとの特徴をもっている。

ここで、図 1 に示す D T V (Digital Television) N 2 の表示部 1 0 及び信号処理部 1 1 は、本来のデジタルテレビの構成であり、外部からの放送信号を受信しこれを復調して映像信号を出力し、これに応じた映像を表示部 1 0 に表示する。

更に、付随する通信機能を用いて、例えば、この映像信号を同期パケットとして、図 7 に示す D V H S N 5 へと、例えば、I E E E 1 3 9 4 の通信規約に応じて送信する。又は、例えば、映像信号の一部である静止画信号を非同期パケットとして、図 7 に示すプリンタ N 6 へと送信する。以下、フローチャートを用いて、送信動作及び受信動作を詳細に説明する。

(送信動作)

初めに、図 5 のフローチャートにおいて、パケット通信を行う対象が同期パケットか、非同期パケットかが判断される(S 1 1)。同期パケットであれば、図 2 に示すように、信号処理部 1 1 から供給された予め決められたブロック長の整数倍の長さの同期パケット P_S が、D T C P 部 1 2 に供給され、ブロック暗号化される(S 1 7)。そして、同期処理部 1 6 により処理された後に、送信部 1 8 を介して、ネットワーク N 上の他の通信装置、例えば、D V H S N 5 へと供給される(S 1 8)。

【0 0 1 2】

一方、パケット通信を行う対象が非同期パケットであると判断されると(S 1 1)、図 2 に示すように、非同期パケットの実データ J がブロック長の整数倍の長さかどうか判断される(S 1 2)。ここで、非同期パケットがブロック長の整

数倍であれば、特にパディング処理を施すことなくそのまま、D T C P 部 1 2 に供給されてブロック暗号化される (S 1 4)。ここで、非同期パケットがブロック長の整数倍でなければ、パディング処理部 1 4 により、パディング処理が施され、図 2 に示すように、非同期パケット P_N は、実データ J に付加データ D が付加されることでパディング処理される。こうしてブロック長の整数倍 (又は 2 倍) の長さに調整され、以降の D T C P 部 1 2 のブロック暗号化に備える (S 1 3)。そして、パディング処理された非同期パケット P_{N2} は、D T C P 部 1 2 に供給され、ブロック暗号化される (S 1 4)。

【 0 0 1 3 】

その後、同期パケットと同様に暗号化された非同期パケット P_{N2} は、図 3 に示すように、データ長情報付加回路 1 7 により、実データ J のデータ長情報 L を、例えば、ヘッダ H の後に付加される (S 1 5)。その後、送信部 1 8 に送られ、ネットワーク N を介して、例えば、プリンタ N 6 に送信される (S 1 6)。

こうすることにより、本発明に係る通信装置によれば、非同期パケットの情報も同期パケットと同様に、ブロック暗号等の暗号化を施してセキュリティを確保しつつ通信処理を行うことが可能となる。

又、更に、図 3 に示すように、非同期パケットに、例えば、D T C P 部 1 2 で暗号化に用いられる暗号鍵をそのまま使用するのではなく、例えば、時間に応じてこの暗号鍵を書き換える鍵書換情報 K に基づき、鍵管理部 1 3 により暗号鍵を書き換えて暗号化を行う。そして、この鍵書換情報 K を、図 3 に示すように、ヘッダ H の後に付加することも好適である。こうすることにより、非同期パケットについても同期パケットと同様に、時変鍵を使用して暗号化を行うことができるため、同期パケットと同様の手法で暗号化・復号処理が可能となる。

なお、鍵書換情報 K は、一例として、時変鍵がいつ変わったかを示す時刻情報であってもよいし、時変鍵が変わったことを示すフラグであってもよく、又、鍵を書き換えるための暗号情報であってもよく、様々な形態が可能である。この鍵書換情報 K は、同期パケットと非同期パケットとで共通していること好適である。

【 0 0 1 4 】

又、更に、パケット情報のコピー回数を、例えば、1回又は0回に制限する等のコピー制御情報Cを、非同期パケット P_{N2} のヘッダHの後に付加することも好適である。このコピー制御情報は、例えば、2ビットの情報により、許容されるコピー回数等を特定している。これにより、非同期パケットについても同期パケットと同様に、コンテンツの複写回数を制限することで、コンテンツの著作権を一定の範囲で保護することが同期パケットと同様の手法で可能となる。

又、更に、図4に示すように、これらのデータ長情報L、鍵書換情報K、コピー制御情報Cの制御情報は、図3に示すように必ずしもヘッダHの後に付加する必要はなく、例えば、データ長情報・コピー制御情報付加回路17の働きにより、制御情報のための専用パケット P_{N3} を用意して、これを、非同期パケット P_{N2} の間に挿入することも好適である。これにより、同様に、非同期パケットも同期パケットと同様の手法により、時変鍵を用いた暗号化・復号処理及びコピー処理の制御を行うことが可能となる。

(受信動作)

このような動作により送信された同期パケット及び非同期パケットは、ネットワークNを介して、他の通信装置により受信され、以下のように受信動作が行われる。

すなわち、図6のフローチャートにおいて、受信部18により通信パケットを受信すると(S21)、同期パケットか非同期パケットかが判断される(S22)。同期パケット P_S であれば、同期処理部16により、ヘッダH等から制御情報を抽出する処理等が施された後に、DTCP部12へと供給され、ブロック暗号により暗号鍵に基づいて復号される。暗号処理が時変鍵を用いられたものであれば、ヘッダH等から抽出された鍵書換情報Kを用いて、暗号化に使用された暗号鍵へと暗号鍵を書き換えた後に、書き換えた暗号鍵を用いて同期パケットを復号する(S26)。そして、復号した同期パケットを信号処理部11へと供給する(S27)。

【0015】

一方、通信パケットが非同期パケットであると判断されると(S22)、非同期パケット P_{N2} をDTCP部12に供給し、ブロック暗号により復号する(S2

3)。暗号処理が時変鍵を用いられたものであれば、鍵管理部 1 3 により、ヘッダ H の後に付加された鍵書換情報 K を用いて、暗号化に使用された暗号鍵へと暗号鍵を書き換えた後に、書き換えた暗号鍵を用いて非同期パケット P_{N2} を復号する。

【 0 0 1 6 】

その後、復号した非同期パケット P_{N2} を非同期処理部／抽出部 1 5 に供給し、ヘッダ H の後に付加されたデータ長情報 L に基づいて、図 2 に示すように、付加データ D を除いた実データ J へと抽出する (S 2 4)。その後、抽出した実データ J を信号処理部 1 1 へと供給する (S 2 5)。

【 0 0 1 7 】

こうすることにより、本発明に係る通信装置によれば、非同期パケットの情報も同期パケットと同様に、ブロック暗号等の復号を施してセキュリティを確保しつつ通信処理を行うことが可能となる。

又、更に、パケット情報のコピー回数を、例えば、1 回又は 0 回に制限する、又は制限なくコピー可能等のコピー制御情報 C が非同期パケット P_{N2} のヘッダ H の後に付加されていれば、信号処理部 1 1 では、このコピー制御情報 C に基づいて、非同期パケット P_{N2} が含むコンテンツである実データ J のコピー制御を行う。これにより、非同期パケットについても同期パケットと同様に、コンテンツの複写回数を制限することで、コンテンツの著作権を一定の範囲で保護することが同期パケットと同様の手法で可能となる。

又、更に、図 4 に示すように、これらのデータ長情報 L、鍵書換情報 K、コピー制御情報 C の制御情報が制御情報のための専用パケット P_{N3} として非同期パケット P_{N2} の間に挿入されて送信されることも可能である。非同期処理部／抽出部 1 5 では、このような専用パケット P_{N3} から各制御情報を取り出し、以降の制御に使用するものである。これにより、同様に、非同期パケットも同期パケットと同様の手法により、時変鍵を用いた暗号化・復号処理及びコピー処理の制御を行うことが可能となる。

以上記載した様々な実施形態により、当業者は本発明を実現することができるが、更にこれらの実施形態の様々な変形例を思いつくことが当業者によって容易

であり、発明的な能力をもたなくとも様々な実施形態へと適用することが可能である。従って、本発明は、開示された原理と新規な特徴に矛盾しない広範な範囲に及ぶものであり、上述した実施形態に限定されるものではない。

【 0 0 1 8 】

【発明の効果】

以上詳述したように本発明によれば、暗号化のブロック長の整数倍ではない非同期パケットも、パディング処理によりデータ長を調整することで、同期パケットと同様の手法により暗号化し復号することができ、これにより、非同期パケットも同期パケットと同様にセキュリティを確保しながら通信処理を行うことができる通信装置を提供することが可能となる。

【図面の簡単な説明】

【図 1】

本発明に係る通信装置であるテレビジョンの構成の一例を示すブロック図。

【図 2】

本発明に係る通信装置により非同期パケットに施されるパディング処理を説明する図。

【図 3】

本発明に係る通信装置によりパディング処理された非同期パケットに制御情報を付加することを説明する図。

【図 4】

本発明に係る通信装置によりパディング処理された非同期パケットに制御情報の専用非同期パケットを付加することを説明する図。

【図 5】

本発明に係る通信装置により非同期パケットをパディング処理して送信処理する動作を説明するフローチャート。

【図 6】

本発明に係る通信装置によりパディング処理された非同期パケットを受信処理する動作を説明するフローチャート。

【図 7】

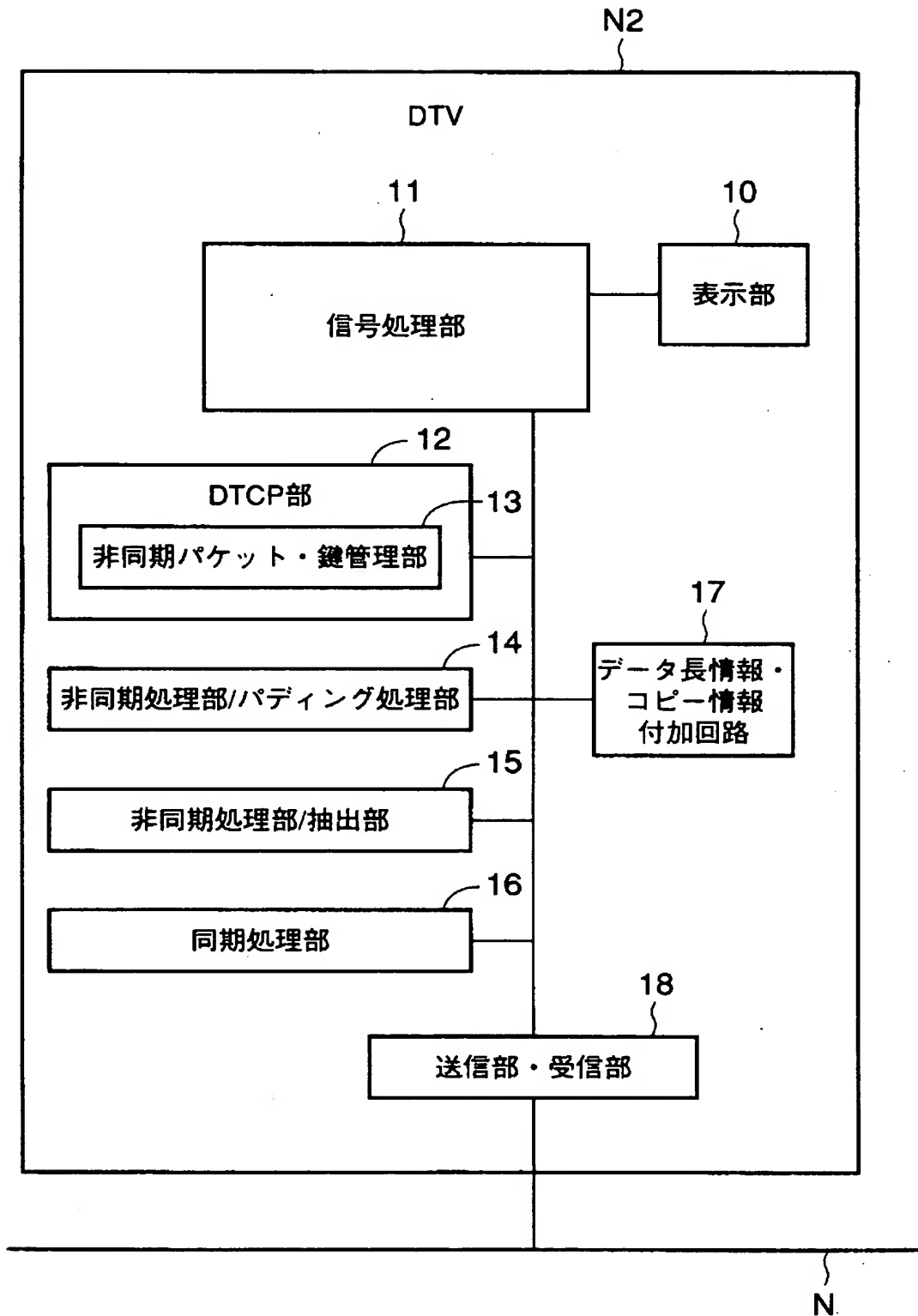
本発明に係る通信装置により構成されたネットワークシステムの一例を示すシステム図。

【符号の説明】

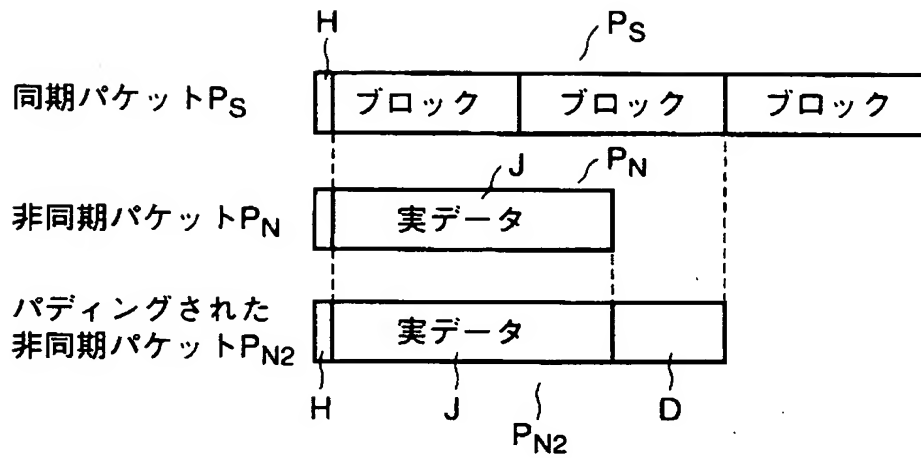
N 2 …通信装置（DTV）、1 0 …表示部、1 1 …信号処理部、1 2 …DTCP部、1 3 …非同期パケット・鍵管理部、1 4 …非同期処理部／パディング処理部、1 5 …非同期処理部／抽出部、1 6 …同期処理部、1 7 …データ長情報・コピー情報付加回路、1 8 …送信部・受信部。

【書類名】 図面

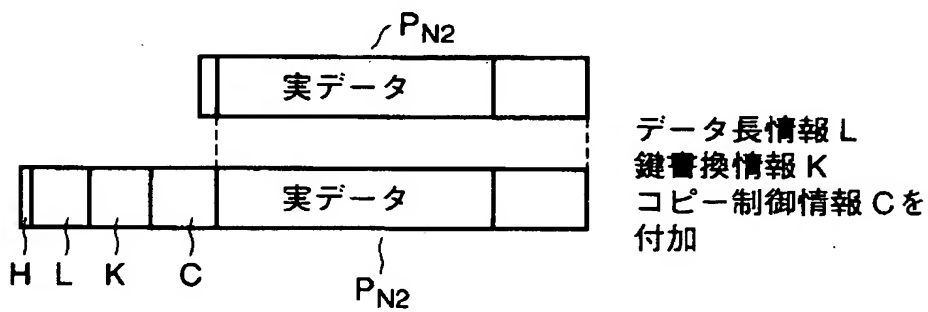
【図 1】



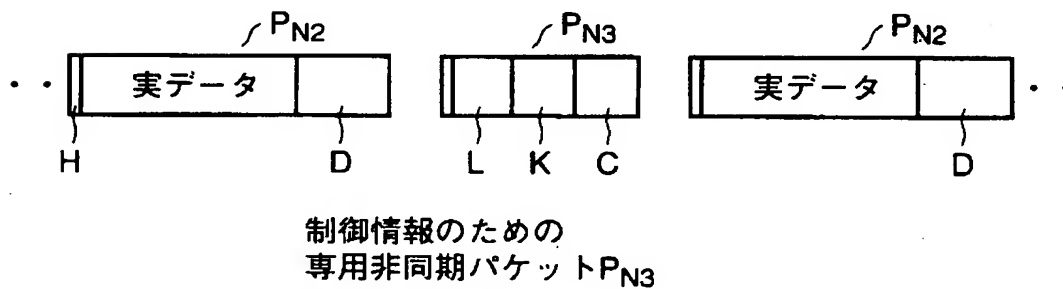
【図 2】



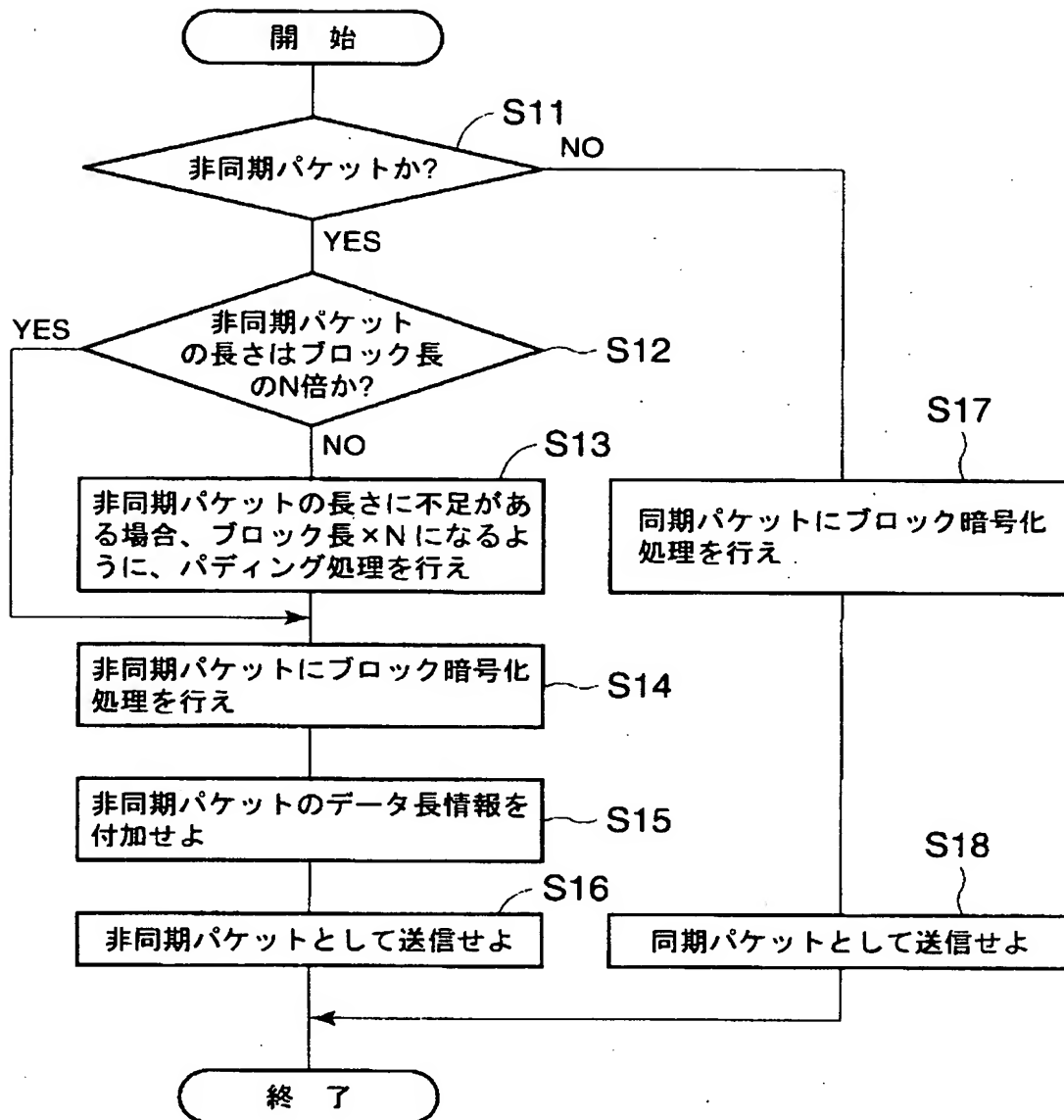
【図 3】



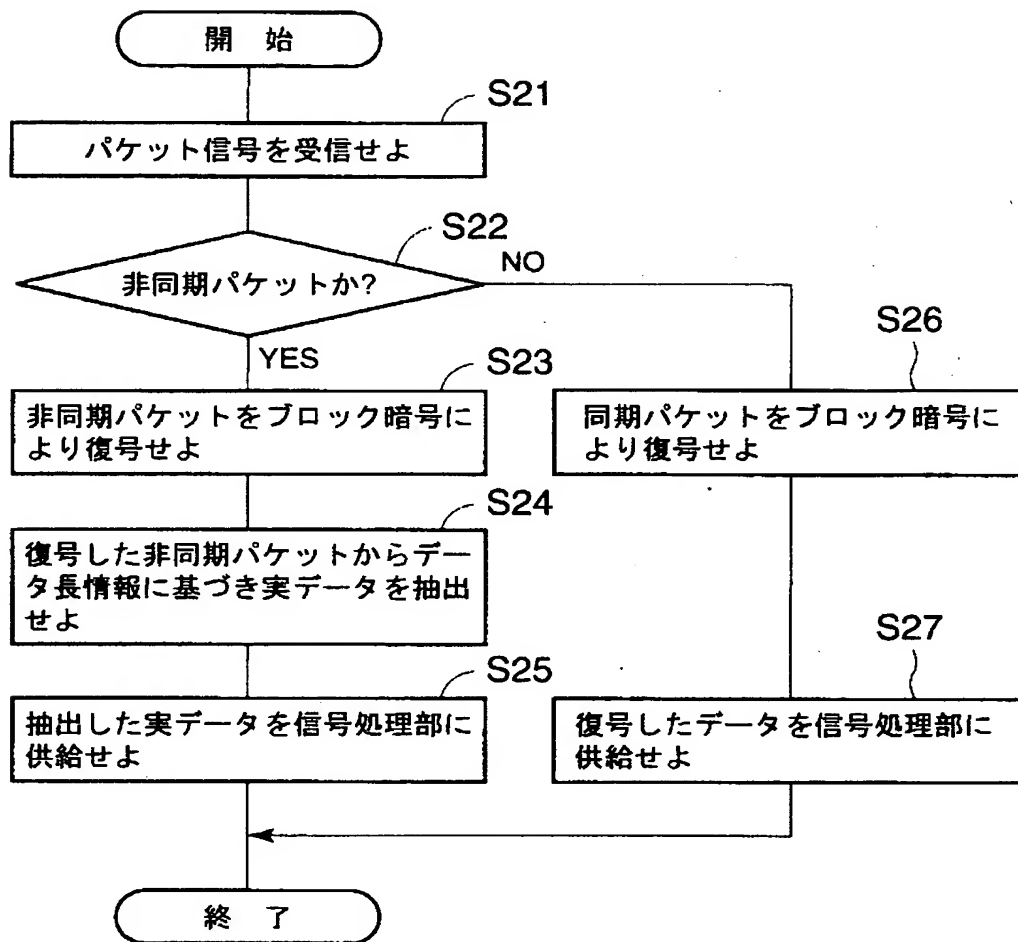
【図 4】



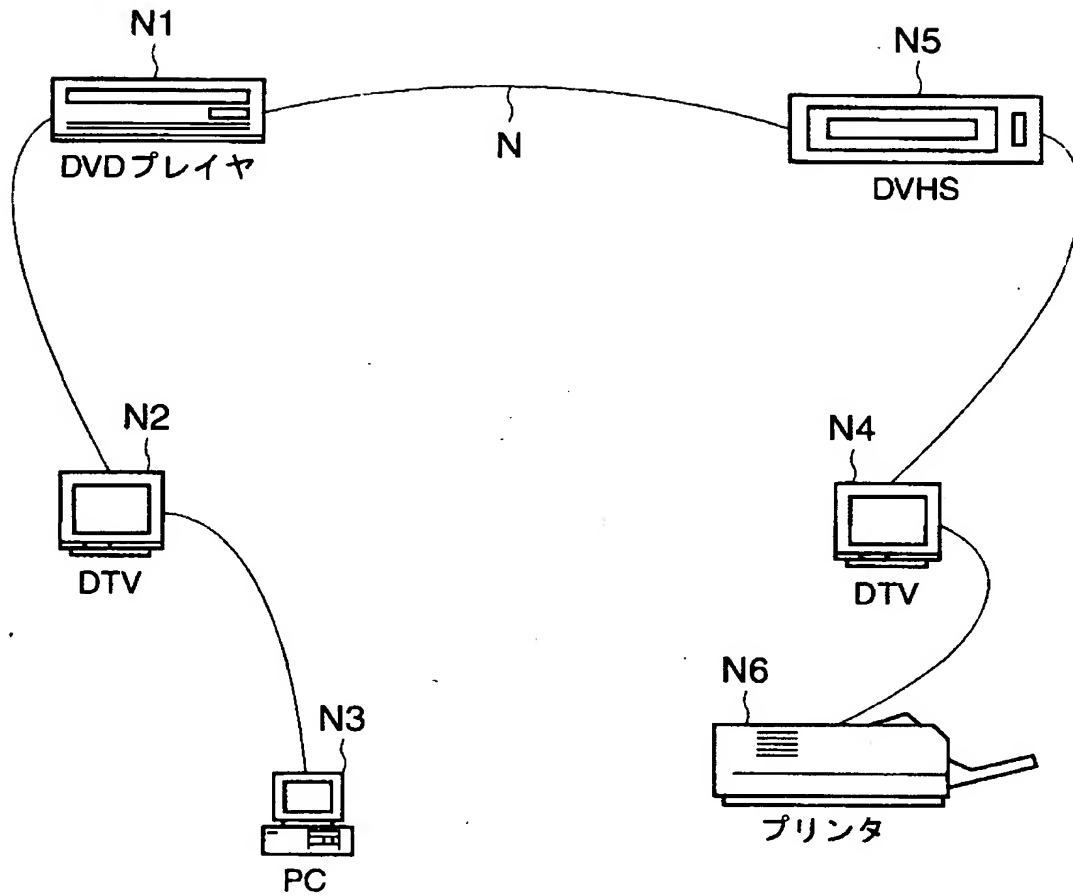
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 非同期パケットも同期パケットと同様に暗号化して通信を行う通信装置及び通信方法を提供する。

【解決手段】 非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施すパディング処理部と、パディング処理部によりパディング処理されたパディング非同期パケット及び同期パケットを暗号化する暗号部と、暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信する送信部とを有する通信装置。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	2001年 7月 2日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目1番1号
氏 名	株式会社東芝